

BEST AVAILABLE COPY**PATENT ABSTRACTS OF JAPAN**

(11)Publication number : 2002-111660

(43)Date of publication of application : 12.04.2002

(51)Int.Cl.

H04L 9/36
H04N 1/387

(21)Application number : 2000-298291

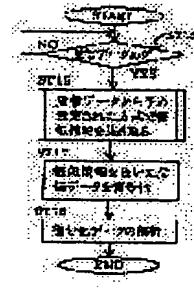
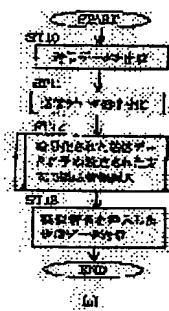
(71)Applicant : TOSHIBA CORP

(22)Date of filing : 29.09.2000

(72)Inventor : SEKIYA SATORU

(54) CRYPTOGRAPHIC COMMUNICATION METHOD AND APPARATUS**(57)Abstract:**

PROBLEM TO BE SOLVED: To provide a cryptographic communication method and apparatus which provides non-significant result even when decoding process is executed.
SOLUTION: When a transmission data is generated for the data to be transmitted or received between an IC card and a reader/writer 4, the encryption process is executed to this transmitting or receiving data. Thereafter, a pseudo information consisting of one or a plurality of non-significant information pieces such as random numbers are inserted to the encrypted data with the preset system which will be explained later and these data are then transmitted (ST10 to 13). Moreover, when the data is received, the pseudo information is extracted from the receiving data with the preset system explained later. Subsequently, the decoding is executed to analyze the decoded data (ST15 to 18).

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C) 1998,2003 Japan Patent Office

(10)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-111660

(P2002-111660A)

(43)公開日 平成14年4月12日 (2002.4.12)

(51) Int CL
H 04 L 9/36
H 04 N 1/387

識別記号

F I
H 04 N 1/387
H 04 L 9/00

テ-マコ-ト(参考)
5 C 07 6
6 8 5 5 J 1 0 4

審査請求 未請求 請求項の数21 O.L (全22頁)

(21)出願番号

特願2000-298291(P2000-298291)

(22)出願日

平成12年9月29日 (2000.9.29)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 関谷 哲

神奈川県川崎市幸区柳町70番地 東芝ソシ
オエンジニアリング株式会社内

(74)代理人 100083161

弁理士 外川 美明

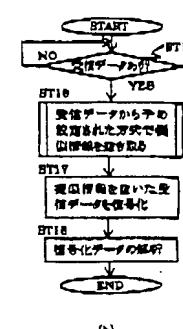
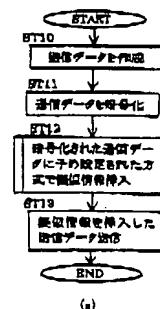
Fターム(参考) 50076 AA09 AA14 BA03 BA05 BA06
BA09
6J104 AA01 JA03 NA07

(54)【発明の名称】 暗号通信方法及び暗号通信装置

(57)【要約】

【課題】 本発明は、暗号化の解説が施されても意味ある結果に達することが極めて困難な暗号通信方法及び暗号通信装置を提供する。

【解決手段】 I Cカード1とリーダライタ4間で送受信される送受信データに対して、送信データを作成すると、暗号化を施した後に、暗号化されたデータに対して後述する予め設定された方式で、乱数等の意味を持たない1つ又は複数の情報からなる擬似情報を挿入し、送信するようになっている (ST10~19)。また、データを受信すると、受信データから後述する予め設定された方式で擬似情報を抜き取った後、復号化を施し、復号化データを解析するようになっている (ST15~18)。



【特許請求の範囲】

【請求項 1】 少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、

送信しようとする情報を暗号化し、この暗号化した送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に挿入して外部装置へ送信し、

前記外部装置から暗号化された情報を受信すると、受信情報から前記擬似情報を除去し、前記擬似情報が除去された受信情報に対して復号化を施すことを特徴とする暗号通信方法。

【請求項 2】 少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、

送信しようとする情報を暗号化し、この暗号化した送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に少なくとも1つ以上挿入し、この挿入した位置を指定する指定情報を送信情報に付加して外部装置へ送信することを特徴とする暗号通信方法。

【請求項 3】 前記挿入した位置を指定する指定情報を送信情報に付与する際、前記指定情報に対して暗号化を施し、この暗号化された指定情報を送信情報に付与することを特徴とする請求項 2 記載の暗号通信方法。

【請求項 4】 前記暗号化した送信情報に対して前記擬似情報を挿入する際、擬似情報の挿入位置を示す複数の法則のうちの少なくとも1つの法則に従って前記擬似情報を挿入することを特徴とする請求項 2 記載の暗号通信方法。

【請求項 5】 前記送信しようとするデータのうち、個人情報が含まれている部分に対してのみ暗号化及び擬似情報の挿入を行うことを特徴とする請求項 2 記載の暗号通信方法。

【請求項 6】 前記外部装置から暗号化された情報を受信すると、受信情報から前記指定情報を抽出し、この抽出された指定情報に従って前記受信情報から前記擬似情報を除去し、前記擬似情報が除去された受信情報に対して復号化を施すことを特徴とする請求項 2 記載の暗号通信方法。

【請求項 7】 少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、外部装置から暗号化された情報を受信すると、受信情報の予め設定された位置から、受信情報とは無関係の擬似情報が挿入された位置を指定する指定情報を抽出し、この抽出された指定情報に従って前記受信情報から前記擬似情報を除去し、前記擬似情報が除去された受信情報に対して復号化を施すことを特徴とする暗号通信方法。

【請求項 8】 前記受信情報から抽出した前記指定情報を復号化し、この復号化した指定情報を従って前記受信情報から前記擬似情報を除去することを特徴とする請求項 7 記載の暗号通信方法。

【請求項 9】 前記受信情報から抽出した前記指定情報に基づいて、擬似情報の挿入位置を示す複数の法則のう

ちの少なくとも1つの法則に従って前記受信情報から前記擬似情報を除去することを特徴とする請求項 7 記載の暗号通信方法。

【請求項 10】 暗号化された情報を送受信する暗号通信装置において、

送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報に対して暗号化を施す暗号化手段と、

この暗号化手段により暗号化された送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に挿入する挿入手段と、

この挿入手段により擬似情報を挿入された送信情報を外部装置に送信する送信手段と、

前記外部装置から送信された情報を受信する受信手段と、

この受信手段により受信された受信情報から前記擬似情報を除去する除去手段と、

この除去手段により擬似情報が除去された受信情報に対して復号化を施す復号化手段とを有することを特徴とする暗号通信装置。

【請求項 11】 暗号化された情報を送受信する暗号通信装置において、

送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報に対して暗号化を施す暗号化手段と、

この暗号化手段により暗号化された送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に挿入する挿入手段と、

この挿入手段により擬似情報を挿入された位置を指定する指定情報を、前記擬似情報を挿入された送信情報に付与して生成された送信情報を外部装置に送信する送信手段と、

を有することを特徴とする暗号通信装置。

【請求項 12】 外部装置から暗号化された情報を受信する受信手段と、

この受信された受信情報の予め設定された位置から、前記指定情報を抽出する抽出手段と、

この抽出された前記指定情報に基づいて前記受信情報から前記擬似情報を除去する除去手段と、

この除去手段により擬似情報が除去された受信情報に対して復号化を施す復号化手段と、

を有することを特徴とする請求項 11 記載の暗号通信装置。

【請求項 13】 暗号化された情報を送受信する暗号通信装置において、

送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報に対して暗号化を施す暗号化手段と、

送信情報とは無関係な擬似情報を生成するため、夫々異なる複数の法則とその法則を指定するための複数の指

(3)

特開2002-111660

3

定情報を記憶する記憶手段と、
前記暗号化手段により暗号化された送信情報に対して上記記憶手段に記憶された法則の少なくとも1つに従って擬似情報を挿入する挿入手段と、
前記擬似情報が挿入された送信情報に対して擬似情報を挿入する際に用いられた前記法則を指定する指定情報を予め設定された位置に付与して、生成された送信情報を外部装置に送信する送信手段と、
を有することを特徴とする暗号通信装置。

【請求項14】 外部装置から暗号化された情報を受信する受信手段と、
この受信された受信情報の予め設定された位置から、前記指定情報を抽出する抽出手段と、
この抽出された前記指定情報に基づいて前記受信情報から前記擬似情報を除去する除去手段と、
この除去手段により擬似情報が除去された受信情報に対して復号化を施す復号化手段と、
を有することを特徴とする請求項13記載の暗号通信装置。

【請求項15】 前記指定情報に対して所定の暗号化を施して前記擬似情報が挿入された送信情報の予め設定された位置に付与する付与手段と、
前記受信手段により受信された受信情報の予め設定された位置から前記暗号化された指定情報を抽出し、この抽出された上記暗号化された指定情報に対して複号化を施す複号化手段と、
をさらに有することを特徴とする請求項12あるいは14記載の暗号通信装置。

【請求項16】 前記指定情報に対して所定の暗号化を施して前記擬似情報が挿入された送信情報の予め設定された位置に付与する付与手段と、
前記受信手段により受信された受信情報の予め設定された位置から前記暗号化された指定情報を抽出し、この抽出された上記暗号化された指定情報に対して複号化を施す複号化手段と、
をさらに有することを特徴とする請求項12あるいは14記載の暗号通信装置。

【請求項17】 複数のアプリケーションプログラムに対応した処理を実行し、暗号化された情報を送受信する暗号通信装置において、
送信情報とは無関係な擬似情報を生成するため、各アプリケーション毎に異なる複数の法則を記憶する記憶手段と、
送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報をに対して暗号化を施す暗号化手段と、
外部装置より指定されたアプリケーションを判別する判別手段と、
前記暗号化手段により暗号化された送信情報に対して、上記記憶手段に記憶された前記判別されたアプリケーションに対応する法則に従って擬似情報を挿入する挿入手段と、
上記擬似情報が挿入された送信情報を外部装置に送信する送信手段と、
を有することを特徴とする暗号通信装置。

4

【請求項18】 前記外部装置から送信された情報を受信する受信手段と、
上記記憶手段に記憶された前記判別されたアプリケーションに対応する法則に従って前記受信情報から前記擬似情報を除去する除去手段と、
この擬似情報が除去された受信情報に対して復号化を施す復号化手段とを有することを特徴とする請求項17記載の暗号通信装置。

【請求項19】 複数のアプリケーションプログラムに対応した処理を実行し、暗号化された情報を送受信する暗号通信装置において、
送信情報とは無関係な擬似情報を生成するため、各アプリケーション毎に異なる複数の法則とその法則を指定するための複数の指定情報を記憶する記憶手段と、
送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報をに対して暗号化を施す暗号化手段と、
外部装置より指定されたアプリケーションを判別する判別手段と、
前記暗号化手段により暗号化された送信情報に対して、上記記憶手段に記憶された前記判別されたアプリケーションに対応する法則に従って擬似情報を挿入する挿入手段と、
前記判別されたアプリケーションに応じて前記送信情報に付与する前記指定情報に暗号化を施すか否かを判断する判断手段と、
この判断手段により暗号化を施すと判断された場合、擬似情報を挿入する際に用いられた前記法則を指定する指定情報を暗号化を施して前記擬似情報が挿入された送信情報に対して付与し、前記判断手段により暗号化は不要と判断された場合には前記指定情報をそのまま前記擬似情報が挿入された送信情報に対して付与する付与手段と、
を有することを特徴とする暗号通信装置。

【請求項20】 所持者に関する情報を記憶した記憶手段を有し、外部装置との間で有線あるいは無線で暗号化された情報を送受信する暗号通信装置において、
送信データと、伝送制御情報と、チェックコードとを所定の送信フォーマットに作成する手段と、
この作成手段により作成された送信情報のうち前記送信データに対して暗号化を施す手段と、
この暗号化手段により暗号化された前記送信データに対して無関係な擬似情報を予め設定された位置に挿入する手段と、
この挿入手段により擬似情報が挿入された送信情報を前記外部装置に送信する手段と、
を有することを特徴とする暗号通信装置。
【請求項21】 所持者に関する情報を記憶した個人情報記憶手段を有し、外部装置との間で有線あるいは無線で暗号化された情報を送受信する暗号通信装置におい

て、
外部装置からの命令に応答して、上記個人情報記憶手段に記憶された所持者に関する情報の少なくとも一部の情報と、伝送制御情報を所定の送信フォーマットに作成する手段と、
この作成された送信情報のうち前記所持者に関する情報で構成された部分に対して暗号化を施す手段と、
この暗号化された送信情報に対して送信情報とは無関係の擬似情報を挿入する夫々異なる複数の法則とその法則を指定するための複数の指定情報を記憶する法則記憶手段と、
上記送信情報の中で前記暗号化された所持者に関する情報に対して前記法則記憶手段に記憶された法則の少なくとも1つに従って擬似情報を挿入する手段と、
この擬似情報が挿入された送信情報に対して擬似情報を挿入する際に使用された法則を指定する指定情報を予め設定された位置に付与して生成された送信情報を送信する手段と、
を有することを特徴とする暗号通信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、暗号通信機能を有する通信装置間、例えば携帯可能な電子装置とそれを扱う情報処理装置間で暗号化が施されたデータを送受信する暗号通信方法及び暗号通信装置に関するもの。

【0002】

【従来の技術】近年、携帯可能な電子装置として、不揮発性のデータメモリとそれを制御するためのCPU(セントラル・プロセッシング・ユニット)を有するICチップを内蔵した、いわゆるICカードが産業各方面で利用されている。また、この種のICカードには、接触式インターフェイスを有する接触式ICカードや、無線等の非接触式インターフェイスを有する無線式ICカードがある。そして、これらICカードは、ICカードに対してデータの読み書きを行なう情報処理装置(例えばリーダライタと称す)を介してデータ通信することにより、オンラインショッピングやホームバンキング等の金融取引にも広く応用されるようになり、通信データを傍受、改ざんされないためのセキュリティ対策が不可欠となってきた。

【0003】このようなセキュリティ対策の手法として、多種多様な暗号化方式が提唱され実用化されている。例えば、特開平10-161535号公報には、通信データに乱数データを付加し所定データサイズ毎にパケット化した後に、パケット単位で暗号化する方法が記載されている。

【0004】

【発明が解決しようとする課題】上述したような従来の装置(方法)では、暗号化する前に乱数データ等を付与しているため、結果的に暗号化方法が解読されてしまつ

た場合には乱数データを含んだ通信データが得られてしまうという問題がある。

【0005】即ち、暗号化方法の解読については、暗号化されたデータを電子計算機を用いて一定の手順で計算を繰り返すことによって最終的に解読されてしまうという問題がある。従来では、このような解読に至るまでの計算量が莫大な量であるため、暗号解読は事実上不可能とされているが、近年の電子計算機の処理能力の飛躍的な向上により、これら暗号化データが現実に解読される可能性が大きくなっている。

【0006】本発明は、以上の点に鑑みられたもので、暗号化の解読が施されても意味ある結果に達することが極めて困難な暗号通信方法、暗号通信装置を提供することを目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明の暗号通信方法は、少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、送信しようとする情報を暗号化し、この暗号化した送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に挿入して外部装置へ送信し、前記外部装置から暗号化された情報を受信すると、受信情報から前記擬似情報を除去し、前記擬似情報が除去された受信情報に対して復号化を施すことを特徴とする。

【0008】また、上記目的を達成するために、本発明の暗号通信方法は、少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、送信しようとする情報を暗号化し、この暗号化した送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に少なくとも1つ以上挿入し、この挿入した位置を指定する指定情報を送信情報に付加して外部装置へ送信することを特徴とする。

【0009】また、上記目的を達成するために、本発明の暗号通信方法は、少なくとも二つの装置間で暗号化された情報を送受信する暗号通信方法において、外部装置から暗号化された情報を受信すると、受信情報の予め設定された位置から、受信情報とは無関係の擬似情報を挿入された位置を指定する指定情報を抽出し、この抽出された指定情報を従って前記受信情報から前記擬似情報を除去し、前記擬似情報が除去された受信情報に対して復号化を施すことを特徴とする。

【0010】上記目的を達成するために、本発明の暗号通信装置は、暗号化された情報を送受信する暗号通信装置において、送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報に対して暗号化を施す暗号化手段と、この暗号化手段により暗号化された送信情報に対して送信情報とは無関係の擬似情報を予め設定された位置に挿入する挿入手段と、この挿入手段により擬似情報が挿入された送信情報を外部装置に送信する送信手段と、前記外部装置から送信された情報

を受信する受信手段と、この受信手段により受信された受信情報から前記擬似情報を除去する除去手段と、この除去手段により擬似情報が除去された受信情報に対して復号化を施す復号化手段とを有することを特徴とする。

【0011】上記目的を達成するために、本発明の暗号通信装置は、複数のアプリケーションプログラムに対応した処理を実行し、暗号化された情報を送受信する暗号通信装置において、送信情報とは無関係な擬似情報を生成するため、各アプリケーション毎に異なった複数の法則を記憶する記憶手段と、送信しようとする情報を所定の送信フォーマット状に作成し、この作成された送信情報に対して暗号化を施す暗号化手段と、外部装置より指定されたアプリケーションを判別する判別手段と、前記暗号化手段により暗号化された送信情報に対して、上記記憶手段に記憶された前記判別されたアプリケーションに対応する法則に従って擬似情報を挿入する挿入手段と、上記擬似情報が挿入された送信情報を外部装置に送信する送信手段と、を有することを特徴とする。

【0012】

【発明の実施の形態】（第1の実施の形態）以下、本発明に係る実施の形態について図面を参照して詳細に説明する。図2は、本発明に係る暗号通信装置としてのICカード1（接触式あるいは無線式ともに含む）及びリーダライタ4（接触式あるいは無線式ともに含む）を用いたシステム構成を説明するための図である。

【0013】図2に示すように、ICカード1を用いたシステムAは、内部メモリ2を有する上位装置としてのホストコンピュータ3、及びこのホストコンピュータ3と接続している端末装置としてのリーダライタ4と、ディスプレイ装置5と、キーボード6とを有している。

【0014】リーダライタ4は内部メモリ4aを有し、ICカード1に対する電文の読み取り、書き込み（送受信）を接触あるいは非接触で行うものである。ディスプレイ装置5は、操作手順や作動状態をオペレーターに知らせるものである。キーボード6は、オペレーターによって操作入力されるものである。

【0015】また、接触式ICカードを用いる場合には、リーダライタ4に接触式ICカードを挿入するためのICカード挿入口部（図示せず）が設けられ、無線式ICカードを用いる場合には、リーダライタ4と無線式ICカードとの間を通信するための通信部（図示せず）が設けられる。

【0016】この様なシステムにより、ICカード1とリーダライタ4間でデータの送受信を行う場合、図1(a)に示すように、例えば、リーダライタ4は、送信データを作成すると(ST10)、暗号化を施した後に(ST11)、暗号化されたデータに対して後述する予め設定された方式で、乱数等の意味を持たない1つ又は複数の情報からなる擬似情報を挿入し(ST12)、通信相手であるICカード1に送信するようになっている。

(ST13)。

【0017】同様に、ICカード1にも上記リーダライタ4と同様の機能(ST10～ST13)を有し、暗号化したデータに予め設定された方式で擬似情報を付加してリーダライタ4に送信することができる。

【0018】また、図1(b)に示すように、例えば、リーダライタ4がICカード1から上記暗号化されたデータを受信すると(ST15)、受信データから後述する予め設定された方式で擬似情報を抜き取った後(ST16)、復号化を施し(ST17)、復号化データを解析するようになっている(ST18)。

【0019】同様に、ICカード1にも上記リーダライタ4と同様の機能(ST15～ST18)を有し、受信した暗号化データから予め設定された方式で擬似情報を抜き取った後、復号化して処理することができる。

【0020】図3は、図2のシステムを構成するリーダライタ4の概略的な制御ブロックを示す図で、図3(a)は接触式ICカードを取り扱うためのリーダライタ4を示し、図3(b)は無線式ICカードを取り扱うためのリーダライタ4を示している。

【0021】図3(a)に示すリーダライタ4は、後述する接触式ICカード1のコンタクト部を介して電気的に接続され、ICカード1と信号の授受を行なうICカードI/F部（インターフェイス）10と、ICカード駆動用の電圧変換回路11と、全体的な制御を司るCPU（セントラル・プロセッシング・ユニット）等を内蔵して構成された制御部12と、電源部としての電池13と、制御プログラムなどを記憶するROM（リード・オンリー・メモリ）14と、ワークメモリに使用する記憶手段としてのRAM（ランダム・アクセス・メモリ）15とから構成している。

【0022】また、図3(b)に示すリーダライタ4は、後述する無線式ICカード1のアンテナ部を介してICカード1と電波信号の授受を行なうICカードI/F部10と、ICカードI/F部を介して送受信される送受信データを変調あるいは復調する変復調回路16と、全体的な制御を司るCPU等を内蔵して構成された制御部12、制御プログラムなどを記憶するROM14と、ワークメモリに使用する記憶手段としてのRAM15とから構成される。

【0023】図4は、図2のシステムを構成するICカード1の機能ブロックを概略的に示す図である。図4に示すように、ICカード1は、リード/ライト部(R/W部)17と、暗証設定/暗証照合部18と、暗号化/復号化部19などの基本機能を実行する部分と、これらの基本機能を管理するスーパーバイザ20とで構成されている。

【0024】R/W部17は、データメモリ等に対してデータの読み出し、書き込み、あるいは消去を行う機能を有する。

【0025】暗証設定／暗証照合部18は、ユーザーが設定した暗証番号の記憶及び読み出し禁止処理を行うと共に、暗証番号の設定後にその暗証番号と外部装置から入力した暗証番号との照合を行い、以後の処理の許可を与える機能を有する。

【0026】暗号化／復号化部19は、例えば、通信回線を介してあるいは無線通信によりリーダライタ4とICカード1との間でデータの送受信を行う場合の通信データの漏洩、偽造を防止するための暗号化や、復号化を行う機能を有する。

【0027】また、暗号化／復号化部19は、暗号化された送信データに対して後述する方法により擬似信号を挿入し、また暗号化されたデータから後述する方法により擬似信号を抜き取り復号化する機能も有する。スーパーパイザ20は、リーダライタ4から入力された機能コード、もしくはデータの付加された機能コードを解読し、実行させる機能を有する。

【0028】図5は、ICカード1の概略的な制御ブロック図を示している。図4に示すように、無線式及び接触式ICカードとともに、図4に示すような諸機能を実行するために、CPU等の制御素子21と、記憶手段としてのデータメモリ22、プログラムメモリ23、ワーカメモリ24、リーダライタ4と信号の授受を行なうI/F部25とから構成されている。

【0029】I/F部25は、無線式ICカード1の場合にはアンテナ部として構成され、リーダライタ4から送信された変調波を非接触で受信したり外部へ変調波を発信するようになっている。また、このアンテナ部25で受信した変調波から内部回路に供給するための電源やクロックを生成するようになっている。

【0030】また、接触式ICカード1の場合にはコンタクト部として構成され、リーダライタ4に設けられた図示せぬICカードI/F部(コンタクト部)と接触することにより電源やクロックを得るようになっている。

【0031】これらの構成のうち、制御素子21、データメモリ22、プログラムメモリ23、及びワーカメモリ24は1つのICチップ(あるいは複数のICチップ)で構成されてICカード本体内に埋設されている。プログラムメモリ23は、例えばマスクROMで構成されており、上述するような各基本機能を実現するサブルーチンを備えた制御素子21の制御プログラム等を記憶している。

【0032】データメモリ22は、アプリケーション及びデータの記憶に使用され、例えばEEPROMなどの消去可能な不揮発性メモリで構成されている。ワーカメモリ24は、制御素子21が処理を行なう際の処理データを一時的に保持するための作業用のメモリであり、例えばRAM等の揮発性メモリで構成されている。

【0033】図6は、データメモリ22の内部構成を示している。データメモリ22は、制御領域220、ディ

レクトリ221、空き領域222、および、エリア群223に分割されている。エリア群223は、複数のデータエリアおよびキーエリアを有することができ、かつ、データファイル(DF)と呼ばれる概念でグループ化することができる。

【0034】また、エリア群223には、送受信間、すなわちリーダライタ4とICカード1で予め取り決めた擬似情報の挿入位置に関する一定の法則が記憶されている。

【0035】図7は、図1に示すST11の送信データの暗号化処理の一例、及び本発明に係るST12の処理の第1の実施の形態に関する具体的な暗号化処理手順を説明する図である。まず、図7(a)乃至(f)は、通常の暗号化処理の手順の一例を示すものである。そして、本発明の第1の実施形態である図7(g)で示す処理を施すことにより、送信データが完成するようになっている。

【0036】図7(a)に示すように、送信したい電文は一般的に、伝送制御情報と、コマンド部やデータ部が含まれたインフォメーション部と、チェックコード部とから構成されている。

【0037】そして、図7(b)に示すように、暗号化する情報として電文のインフォメーション部を、シリアルなデジタルデータで表現し、それを一定の長さ(例えば16ビット)づつのブロックに等分する。この際、端数が生じたら、末尾のブロックが所定長(例えば16ビット)になるまで空白部分を予め定められた値(例えば"0")で埋めていく。

【0038】次に、図7(d)に示すようなリーダライタ4とICカード1とで予め取り決めた暗号化キーと、各ブロック内の値(例えば図7(c)のように)とを一定の手順、例えば排他的論理和演算等で計算処理することにより、図7(e)乃至図7(f)に示す状態で、通常の暗号化処理が終了する。

【0039】本発明の第1の実施の形態では、図7(f)に示すような計算処理の結果に対して、リーダライタ4とICカード1との間で予め取り決めてある一定の位置に擬似情報X1、X2を、図7(g)に示すように挿入する。このように作成された電文に対して、伝送制御情報とチェックコード部が付与されることにより、送信用の暗号化済み電文(図7(h))が形成されるようになっている。尚、伝送制御情報を暗号化しないのは、この部分を暗号化してしまうと電文の伝送が正常に行なわれなくなるためである。

【0040】このような暗号化処理方法を実施した場合のICカード1とリーダライタ4間のデータ通信について、図8を用いて説明する。図8は、図2乃至図6に示すようなICカード1とリーダライタ4で構成されるシステムにおいて、図7に示すような暗号化処理方法を実施した場合のデータ処理を説明するためのフローチャー

50

ト図である。

【0041】まず、リーダライタ4からICカード1へデータを送信する場合、リーダライタ4の制御部12は、送信データを作成し(ST10a)、暗号化を施す(ST11a)。その後、暗号化されたデータに対して、ROM15(あるいはRAM14)に記憶した図7に示す暗号化処理方式で、乱数等の意味を持たない1つ又は複数の情報からなる擬似情報X1、X2を挿入し(ST12a)、ICカード1/F部10を介してICカード1に送信するようになっている(ST13a)。

【0042】ICカード1のCPU21は、I/F部25を介してリーダライタ4から上記暗号化されたデータを受信すると(ST15b)、受信データから図7に示す暗号化処理方法に基づいて擬似情報X1、X2を抜き取る(ST16b)。その後、復号化を施し(ST17b)、復号化データを解析するようになっている(ST18b)。

【0043】また、ICカード1からリーダライタ4へデータを送信する場合、ICカード1のCPU21は、送信データを作成し(ST10b)、暗号化を施す(ST11b)。その後、暗号化されたデータに対して、ROM23(あるいはEEPROM22)に記憶した図7に示す暗号化処理方式で、乱数等の意味を持たない1つ又は複数の情報からなる擬似情報X1、X2を挿入し(ST12b)、I/F部25を介してリーダライタ4に送信するようになっている(ST13b)。

【0044】リーダライタ4の制御部12は、ICカード1/F部10を介してICカード1から上記暗号化されたデータを受信すると(ST15a)、受信データから図7に示す暗号化処理方法に基づいて擬似情報X1、X2を抜き取る(ST16a)。その後、復号化を施し(ST17a)、復号化データを解析するようになっている(ST18a)。

【0045】以上のように、第1の実施の形態では、リーダライタ4から外部装置(ICカード1)へ、あるいはICカード1から外部装置(リーダライタ4)へデータを送信する際に、データを暗号化した上に、更に暗号化されたデータに対して、予め設定してある位置に乱数等の意味を持たない1つ又は複数の情報からなる擬似情報を挿入することによって送信データを作成し、外部装置へ送信するようになっている。

【0046】また、第1の実施の形態では、外部から暗号化データを受信したICカード1あるいはリーダライタ4は、受信データから予め設定された位置にある擬似情報を抜き取った後、復号化を実行するようになっている。

【0047】従って、第1の実施の形態では、暗号化を解説する前に、予め設定された条件に従って正確に擬似情報を取り出さなければ、暗号化の解説が施されても意味ある結果に達することが極めて困難となり、セキュリ

ティを高いデータ通信を維持することが可能となるという効果を奏する。

【0048】(第1の変形例) 次に、図9は、第1の実施の形態における暗号化処理方法の第1の変形例に関する具体的な暗号化処理手順を説明する図である。図9

(a)乃至(f)は、通常の暗号化処理の手順の一例を示すものである。そして、図9(g)及び(h)で示す処理を施すことにより、本発明の送信データが完成するようになっている。

【0049】尚、図9(a)乃至(h)までの処理は、図7に示す第1の実施の形態と同様である。即ち、送信したい電文のインフォメーション部を、シリアルなデジタルデータで表現し、16ビットづつのブロックに等分し、予め取り決められた一定の法則に従って、暗号化キーと各ブロック内の値とに所定の計算処理を施し、図9(e)乃至(f)に示す状態で、通常の暗号化処理が終了する迄は同様である。

【0050】この第1の変形例では、暗号化されたデータ部に対して挿入される擬似情報の挿入位置(挿入法則)が、図10に示すように、複数通り予め設定されており、リーダライタ4のメモリ4a及びICカード1のデータメモリ22に記憶されている。そして、擬似情報を挿入する際に、挿入位置を決定し、擬似情報を挿入後、挿入した位置(法則)をあらわす指定情報Yを送信データに付与するようになっている。

【0051】即ち、図9(f)に示すような計算処理の結果に対して、図10に示す中から選択した位置(法則)に従って、所定の位置(ブロック間)に擬似情報X1、X2を挿入する。次に、図9(g)に示すように、作成された電文に対して、更に指定情報Yを付加することにより、図9(h)に示すように、送信用の暗号化済み電文が形成されるようになっている。

【0052】また、データを受信した装置(ICカード1あるいはリーダライタ4等)は、受信データ中の所定位置に付与された指定情報Yに基づいて、装置内部のメモリ(リーダライタ4のメモリ4aあるいはICカード1のデータメモリ22等)に記憶されている図10に示すようなテーブルから擬似情報X1、X2の挿入位置を判断する。そして、指定情報Yに基づいて判断された挿入位置から擬似情報X1、X2を抜き取り、その後、復号化を実行して復号化データを解析するようになる。

【0053】以上のように、第1の実施の形態の第1の変形例では、暗号化されたデータ部に対する擬似情報の挿入位置(挿入法則)を複数通り有しており、選択した挿入位置に擬似情報を挿入し、かつ挿入した位置(法則)をあらわす指定情報Yを送信データに付与するようになっている。

【0054】また、外部から暗号化データを受信したICカード1あるいはリーダライタ4は、受信データに含まれている指定情報Yに基づいて複数の法則の中から擬

似情報の挿入位置を選択し、選択した位置から擬似情報を抜き取り、復号化を実行するようになっている。

【0055】従って、第1の変形例では、予め設定された条件に従って正確に擬似情報を取り出さなければならぬ上、この条件が複数通り設けられているため、擬似情報の挿入位置が解析されにくく、よりセキュリティの高いデータ通信を維持することが可能となるという効果を奏する。

【0056】(第2の変形例) 次に、図11は、第1の実施の形態における暗号化処理方法の第2の変形例に関する具体的な暗号化処理手順を説明する図である。図11(a)乃至(f)は、通常の暗号化処理の手順の一例を示すものである。そして、図11(g)及び(h)で示す処理を施すことにより、本発明の送信データが完成するようになっている。

【0057】尚、図11(a)乃至(g)までの処理は、図7に示す第1の実施の形態及び図9に示す第1の変形例と同様である。即ち、送信したい電文のインフォメーション部を、シリアルなデジタルデータで表現し、16ビットづつのブロックに等分し、予め取り決められた一定の法則に従って、暗号化キーと各ブロック内の値とに所定の計算処理を施し、図11(e)乃至(f)に示す状態で、通常の暗号化処理が終了する迄は同様である。

【0058】この第2の変形例では、第1の変形例と同様に暗号化されたデータ部に対して挿入される擬似情報の挿入位置(挿入法則)が、図10に示すように、複数通り予め設定されており、複数通りの中から挿入位置を決定し、擬似情報を挿入した後、さらに暗号化を施した指定情報Yを送信データに付与するようになっている。

【0059】即ち、図11(f)に示すような計算処理の結果に対して、図10に示す中から選択した位置(法則)に従って、所定の位置(ブロック間)に擬似情報X1、X2を挿入する。次に、図10に示す擬似情報の挿入位置(法則)を示す指定情報Yに対して所定の暗号化処理を施し、図11(g)に示す擬似情報X1、X2が挿入された電文に対して、暗号化した指定情報Y'を附加することにより、図11(h)に示すように、送信用の暗号化済み電文が形成されるようになっている。

【0060】また、データを受信した装置(I Cカード1あるいはリーダライタ4等)は、受信データ中の所定位置に付与された暗号化された指定情報Y'を抜き取り、復号化を施し、指定情報Yを得る。復号化した指定情報Yに基づいて、装置内部のメモリ(リーダライタ4のメモリ4&あるいはI Cカード1のデータメモリ22等)に記憶されている図10に示すようなテーブルから擬似情報X1、X2の挿入位置を判断する。そして、指定情報Yに基づいて判断された挿入位置から擬似情報X1、X2を抜き取り、その後、復号化を実行して復号化データを解析するようになる。

【0061】以上のように、第1の実施の形態の第2の変形例では、擬似情報の挿入位置が複数通り設けられている上に、送信データに付与された挿入位置に指定情報が暗号化されているため、擬似情報の挿入位置自体を解読することがより困難となりセキュリティの高いデータ通信を維持することが可能となるという効果を奏する。

【0062】(第3の変形例) 次に、図12は、第1の実施の形態における暗号化処理方法の第3の変形例に関する具体的な暗号化処理手順を説明する図である。図12(a)乃至(f)は、通常の暗号化処理の手順の一例を示すものである。そして、図12(g)及び(h)で示す処理を施すことにより、本発明の送信データが完成するようになっている。

【0063】本発明の第3の変形例では、第1の実施の形態、第1及び第2の変形例において電文のコマンド部(コマンド及びコマンドパラメータで構成)やデータ部が含まれたインフォメーション部に対して暗号化処理及び擬似情報の挿入処理を実行していたのに対して、コマンド部は暗号化処理せず、データ部のみに対して暗号化処理及び擬似情報の挿入処理を実行するようにしたものである。

【0064】尚、データ部のみに対して暗号化処理及び擬似情報の挿入処理を実行する以外は、図12(a)乃至(g)までの処理は、図7に示す第1の実施形態と同様である。即ち、送信したい電文のデータ部を、シリアルなデジタルデータで表現し、16ビットづつのブロックに等分し、予め取り決められた一定の法則に従って、暗号化キーと各ブロック内の値とに所定の計算処理を施し、図9(e)乃至(f)に示す状態で、通常の暗号化処理が終了する。

【0065】第3の変形例では、図12(f)に示すような計算処理の結果に対して、リーダライタ4とI Cカード1との間で予め取り決めてある一定の位置に擬似情報X1、X2を挿入する。このように作成された電文(図12(g))に対して、伝送制御情報、コマンド部、及びチェックコード部が付与されることにより、送信用の暗号化済み電文が形成されるようになっている。

【0066】尚、伝送制御情報を暗号化しないのは、この部分を暗号化してしまうと電文の伝送が正常に行なわれなくなるためであり、コマンド部を暗号化しないのは、コマンド部には個人情報等の秘密情報は含まれていないためである。

【0067】また、データを受信した装置(I Cカード1あるいはリーダライタ4等)は、受信データ中の伝送制御情報、コマンド部、及びチェックコード部以外の部分に対して、次の処理を施す。まず、予め設定されている挿入位置から擬似情報X1、X2を抜き取り、その後、復号化を実行して復号化データを解析するようになる。

【0068】以上のように、第1の実施の形態の第3の

変形例では、送信データの中でデータ通信共通に用いられる伝送制御情報、コマンド部、及びチェックコード部以外の部分に対してのみ暗号化を実施後、擬似情報を挿入しており、円滑にデータ通信処理を実行でき、かつセキュリティが高いデータ通信を維持することが可能となるという効果を奏する。

【0069】(第4の変形例) 次に、図13は、第1の実施の形態における暗号化処理方法の第4の変形例に関する具体的な暗号化処理手順を説明する図である。

【0070】この第4の変形例では、第1の変形例において電文のコマンド部やデータ部が含まれたインフォメーション部に対して暗号化処理、擬似情報の挿入処理、及び指定情報Yの付加を実行していたのに対して、コマンド部は暗号化処理せず、データ部のみに対して暗号化処理、擬似情報X1、X2の挿入処理、及び指定情報Yの付加を実行するようにしたものである。それ以外は、第1の実施の形態及び第1の変形例と同様であるため、説明を省略する。

【0071】以上のように、第1の実施の形態の第4の変形例では、送信データの中でデータ通信共通に用いられる伝送制御情報、コマンド部、及びチェックコード部以外の部分に対してのみ暗号化を実施後、擬似情報を挿入し、また挿入位置も複数通りから選択できるようになっているため、円滑にデータ通信処理を実行できるばかりか、セキュリティが高いデータ通信を維持することが可能となるという効果を奏する。

【0072】(第5の変形例) 次に、図14は、第1の実施の形態における第5の変形例に関する具体的な暗号化処理手順を説明する図である。

【0073】第3及び第4の変形例においては、電文のインフォメーション部を構成するデータ部に対して暗号化処理、擬似情報X1、X2の挿入処理、及び指定情報Yの付加等を実行していた。

【0074】これに対して、この第5の変形例では、コマンド部及び個人情報以外のデータ部は暗号化処理せず、データ部の中でもセキュリティの高いデータ(例えば、暗証番号や金額情報等)に該当する個人情報部分のみに対して暗号化処理、擬似情報X1、X2の挿入処理、及び暗号化した指定情報Y'の付加を実行するようにしたものである。それ以外は、第2の変形例と同様であるため、説明を省略する。

【0075】従って、第1の実施の形態の第5の変形例では、送信データの中でセキュリティの高い部分のデータにのみ、暗号化して擬似情報を挿入し、更には挿入位置も複数通りから選択できるようになっており、指定情報をも暗号化して付与しているため、円滑にデータ通信処理を実行できるばかりか、セキュリティを高いデータ通信を維持することが可能となるという効果を奏する。

【0076】(第2の実施の形態) 次に、本発明に係る第2の実施の形態について図面を参照して詳細に説明す

る。本実施の形態では、ICカード1のデータメモリ22には、複数のアプリケーションが記憶されており、またリーダライタ4も複数のアプリケーションを取り扱い可能なシステム構成であり、アプリケーションに求められるセキュリティレベルに応じて、擬似情報X1、X2のデータ量を可変設定できるようになっている。

【0077】尚、電文のインフォメーション部あるいはデータ部の暗号化方法、擬似情報の挿入方法は上述した第1の実施の形態及び第3の変形例と同様であるため、説明を省略する。

【0078】図15は、リーダライタ4のメモリ4a、あるいはICカード1のデータメモリ22に記憶されたアプリケーション毎の暗号処理設定テーブルである。

【0079】図15に示すように、本実施の形態では、リーダライタ4及びICカード1には複数のアプリケーションとして、クレジットカード、ポイントカード、及びプリペイドカードとしてのアプリケーションが記憶されている。そして、複数あるアプリケーションのセキュリティレベルは、プリペイドカードアプリが最も低く、次に個人情報を含むポイントカードアプリ、より個人情報等の秘密情報を含むクレジットカードが最も高く設定されている。

【0080】従って、本実施の形態では、クレジットカードアプリにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、2バイト毎に擬似情報を挿入するように設定される。また、ポイントカードアプリにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、6バイト毎に擬似情報を挿入するように設定される。

【0081】また、プリペイドカードにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、10バイト毎に擬似情報を挿入するように設定され、セキュリティレベルに応じて擬似情報のデータ量を可変としている。

【0082】図16は第2の実施の形態における制御フローチャートを示す図である。リーダライタ4とICカード1との間の処理で実行するアプリケーションが指定されると(ST20)、リーダライタ4はメモリ4aから、ICカード1はデータメモリ22から、指定されたアプリケーションに対応した暗号化方法(何バイト毎に擬似情報の挿入するか)を読み出し設定する(ST21)。

【0083】ST21の状態で、送信データがある場合には(ST22)、リーダライタ4あるいはICカード1は、送信データ中にICカード1の所持者に関連する個人情報が含まれているかを判定する(ST23)。ST23で個人情報が含まれている場合、送信データ(あるいは個人データのみ)を暗号化し、この暗号化されたデータに対して、ST21で読み出し設定したバイト数毎に擬似情報を挿入した後(ST24)、データ送信を

(10)

17

実行する (ST 25)。

【0084】また、ST 22でデータを受信した場合には、リーダライタ4あるいはICカード1は、受信データからST 21で読み出し設定されたバイト数ごとに擬似情報を抜き出した後 (ST 27)、復号化を行ない、復号化データの解析を実行する (ST 28)。

【0085】従って、第2の実施の形態では、アプリケーションのセキュリティレベルに応じて挿入する擬似情報のデータ量を可変設定することができる。これにより、所定の装置以外を用いた擬似情報の抜き取りは極めて困難となり、予め設定された条件に従って正確に擬似情報を取り出さなければ、暗号化の解読が施されても意味ある結果に達することが極めて困難となり、セキュリティを高いデータ通信を維持することが可能となるという効果を奏する。

【0086】(第3の実施の形態) 次に、本発明に係る第3の実施の形態について図面を参照して詳細に説明する。本実施の形態においても、第2の実施の形態と同様に、ICカード1のデータメモリ22には、複数のアプリケーションが記憶されており、またリーダライタ4も複数のアプリケーションを取り扱い可能なシステム構成であり、アプリケーションに求められるセキュリティレベルに応じて、擬似情報の挿入位置(法則)が設定されている。

【0087】尚、電文のインフォメーション部あるいはデータ部の暗号化方法、擬似情報の挿入方法、指定情報の付加は上述した第1の実施の形態及び第3の変形例と同様であるため、説明を省略する。

【0088】図17は、リーダライタ4のメモリ4a、あるいはICカード1のデータメモリ22に記憶されたアプリケーション毎の暗号処理設定テーブルである。

【0089】本実施の形態では、第2の実施の形態と同様に、リーダライタ4及びICカード1には複数のアプリケーションとして、クレジットカード、ポイントカード、及びプリペイドカードのアプリケーションが記憶されている。そして、セキュリティレベルがプリペイドカードアプリが最も低く、次に個人情報を含むポイントカードアプリ、より個人情報等の秘密情報を含むクレジットカードが最も高く設定されている。

【0090】従って、本実施の形態では、クレジットカードアプリにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、素数番目のブロックの後に擬似情報を挿入することを意味した指定情報Y=「3」に設定され、不規則に擬似情報が挿入される法則を選択している。また、指定情報Yは暗号化するよう設定されている。

【0091】ポイントカードアプリにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、奇数番目のブロックの後に擬似情報を挿入することを意味した指定情報Y=「1」に設定され、規則的に擬

特開2002-111660

18

似情報が挿入される法則を選択している。また、指定情報Yは暗号化しないよう設定されている。

【0092】また、プリペイドカードにてリーダライタ4とICカード1間でデータの送受信が行なわれる場合には、4の整数倍のブロックの後に擬似情報を挿入することを意味した指定情報Y=「6」に設定され、挿入される擬似情報が少ない法則を選択している。また、指定情報Yは暗号化しないよう設定されている。

【0093】このように、セキュリティレベルに応じて擬似情報の挿入方法を選択し、一緒に送付する指定情報の暗号化の要否も選択するようにしている。

【0094】図18は、第3の実施の形態における制御フローチャートを示す図である。リーダライタ4とICカード1との間の処理で実行するアプリケーションが指定されると (ST 30)、リーダライタ4はメモリ4aから、ICカード1はデータメモリ22から、指定されたアプリケーションに対応した指定情報及び指定情報の暗号化の要否を読み出し設定する (ST 31)。

【0095】ST 31の状態で、送信データがある場合には (ST 32)、リーダライタ4あるいはICカード1は、送信データを暗号化し (ST 33)、この暗号化されたデータに対して、ST 31で読み出し設定した指定情報で予め決められた法則に沿って擬似情報を挿入する (ST 34)。

【0096】次にST 31で指定情報を暗号化するよう設定されている場合には (ST 35)、指定情報を暗号化して送信データに付与し (ST 36)、データ送信を実行する (ST 37)。また、ST 31で指定情報を暗号化しないよう設定されている場合には (ST 35)、指定情報は暗号化せずに送信データに付与し、データ送信を実行する (ST 37)。

【0097】ST 31の状態で、データを受信した場合には (ST 32)、リーダライタ4あるいはICカード1は、ST 31の設定で指定情報は暗号化するか否かを判定し (ST 40)、指定情報を暗号化するよう設定されている場合には、指定情報を復号化し (ST 41)、指定情報を暗号化しないよう設定されている場合には受信データの電文中の所定の位置から指定情報を取り出す。次に、受信データから指定情報で予め設定された法則に沿って擬似情報を抜き出した後 (ST 42)、復号化を行ない、復号化データの解析を実行する (ST 43)。

【0098】従って、第3の実施の形態では、アプリケーションのセキュリティレベルに応じて挿入する擬似情報のデータ量を可変設定することができ、更には指定情報の暗号化の可否をも設定可能となっている。これにより、所定の装置以外を用いた擬似情報の抜き取りは極めて困難となり、予め設定された条件に従って正確に擬似情報を取り出さなければ、暗号化の解読が施されても意味ある結果に達することが極めて困難となり、セキュリ

(11)

19

ティを高いデータ通信を維持することが可能となるという効果を奏する。

【0099】

【発明の効果】以上説明したように、本発明によれば、暗号化の解読が施されても意味ある結果に達することが極めて困難とすることができます。

【図面の簡単な説明】

【図1】本発明に係る暗号通信方法を説明するためのフローチャート図。

【図2】ICカード1及びリーダライタ4を用いたシステム構成Aを概略的に説明するための図。

【図3】リーダライタ4の基本的な制御ブロックを示す図。

【図4】ICカード1の基本的な機能ブロックを示す図。

【図5】ICカード1の制御ブロックを示す図。

【図6】ICカード1のデータメモリ22の構成を概念的に説明するための図。

【図7】図1に示すST11の送信データの暗号化処理の一例、及び本発明に係るST12の処理の第1の実施の形態について、具体的な暗号化処理手順を説明する図。

【図8】本発明に係る暗号通信方法を用いたリーダライタ4とICカード1間のデータ通信を説明するためのフローチャート図。

【図9】第1の実施の形態における第1の変形例についての具体的な暗号化処理手順を説明する図。

【図10】リーダライタ4のメモリ4a及びICカード

(11)

特開2002-111660

20

1のデータメモリ22に予め記憶され、暗号化されたデータ部に対して挿入される擬似情報の挿入位置(挿入法則)を説明する図。

【図11】第1の実施の形態における第2の変形例についての具体的な暗号化処理手順を説明する図。

【図12】第1の実施の形態における第3の変形例についての具体的な暗号化処理手順を説明する図。

【図13】第1の実施の形態における第4の変形例についての具体的な暗号化処理手順を説明する図。

【図14】第1の実施の形態における第5の変形例についての具体的な暗号化処理手順を説明する図。

【図15】本発明に係る暗号通信方法の第2の実施の形態における、リーダライタ4のメモリ4a、あるいはICカード1のデータメモリ22に記憶されたアプリケーション毎の暗号処理設定テーブルを概略的に示す図。

【図16】本発明に係る暗号通信方法の第2の実施の形態を説明するためのフローチャート図。

【図17】本発明に係る暗号通信方法の第3の実施の形態における、リーダライタ4のメモリ4a、あるいはICカード1のデータメモリ22に記憶されたアプリケーション毎の暗号処理設定テーブルの他の実施形態を概略的に示す図。

【図18】本発明に係る暗号通信方法の第3の実施の形態を説明するためのフローチャート図。

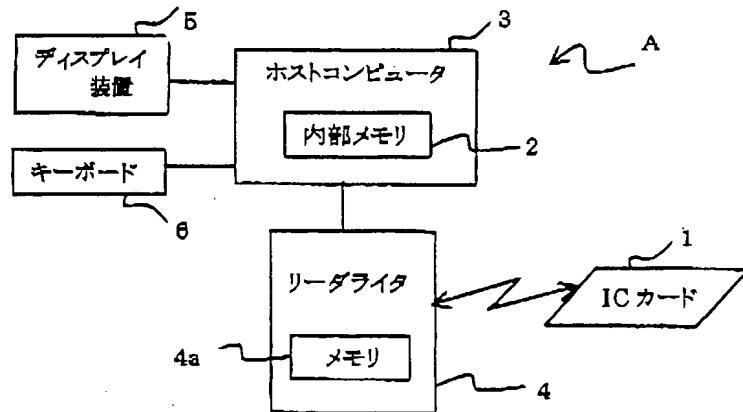
【符号の説明】

A システム

1 ICカード

4 リーダライタ

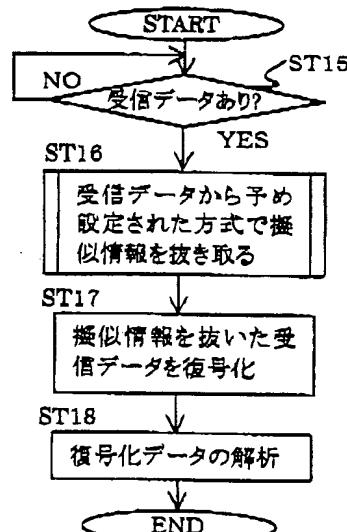
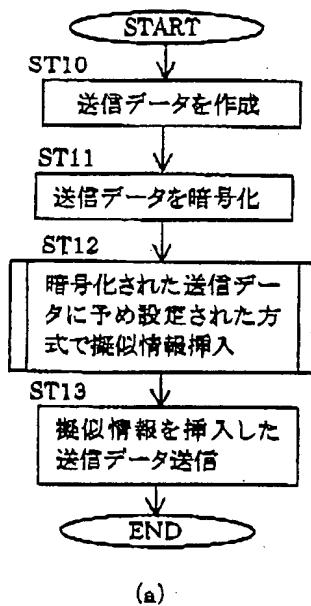
【図2】



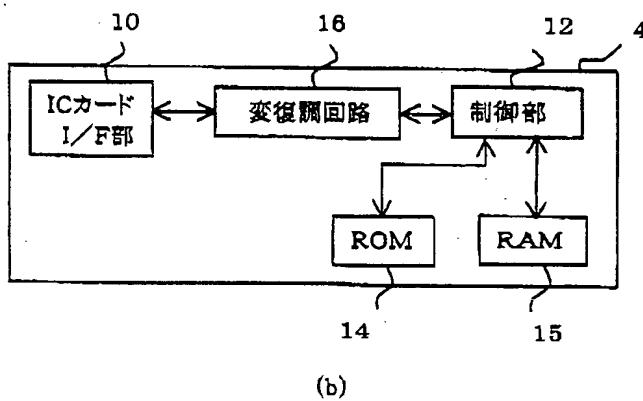
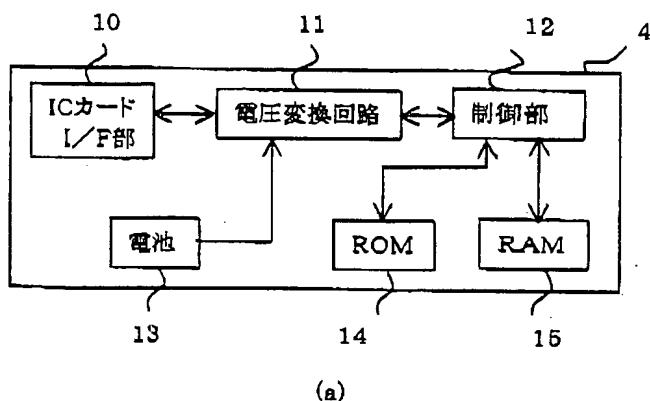
(12)

特開2002-111660

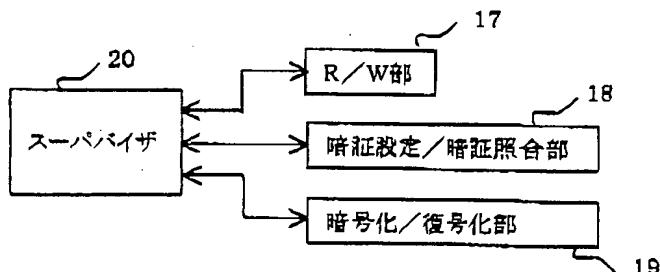
【図1】



【図3】



【図4】



【図15】

アプリケーション	擬似情報の挿入
クレジットカード	2バイト
ポイントカード	6バイト
プリペイドカード	10バイト

223

223a

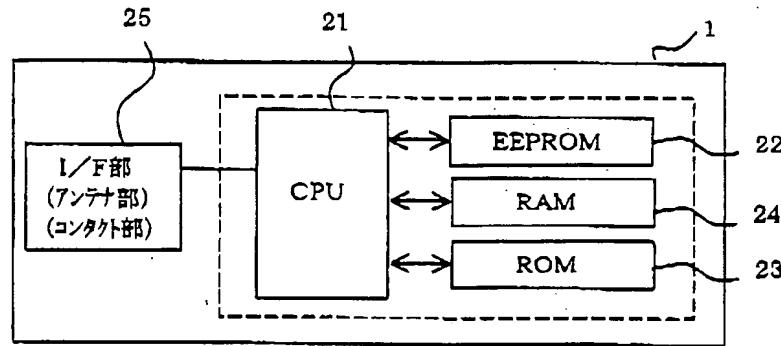
223b

223c

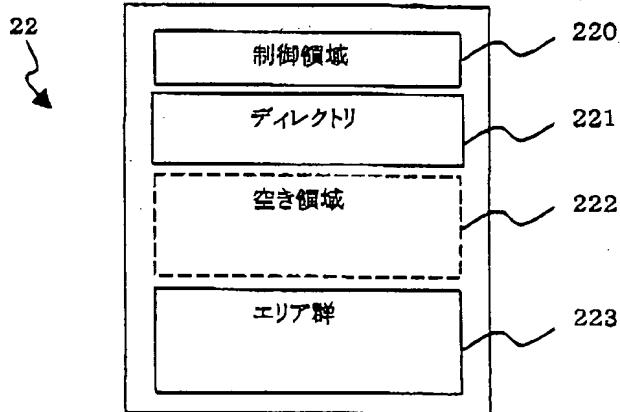
(13)

特開2002-111660

【図5】



【図6】



【図10】

指定情報	擬似情報(X1, X2, ...)を挿入する法則
1	奇数番目のブロックの後に挿入
2	偶数番目のブロックの後に挿入
3	素数番目(1, 2, 3, 7, 11, ...)のブロックの後に挿入
4	3の整数倍(3, 6, 9, ...)のブロックの後に挿入
5	4の整数倍(4, 8, 12, ...)のブロックの後に挿入
...	...

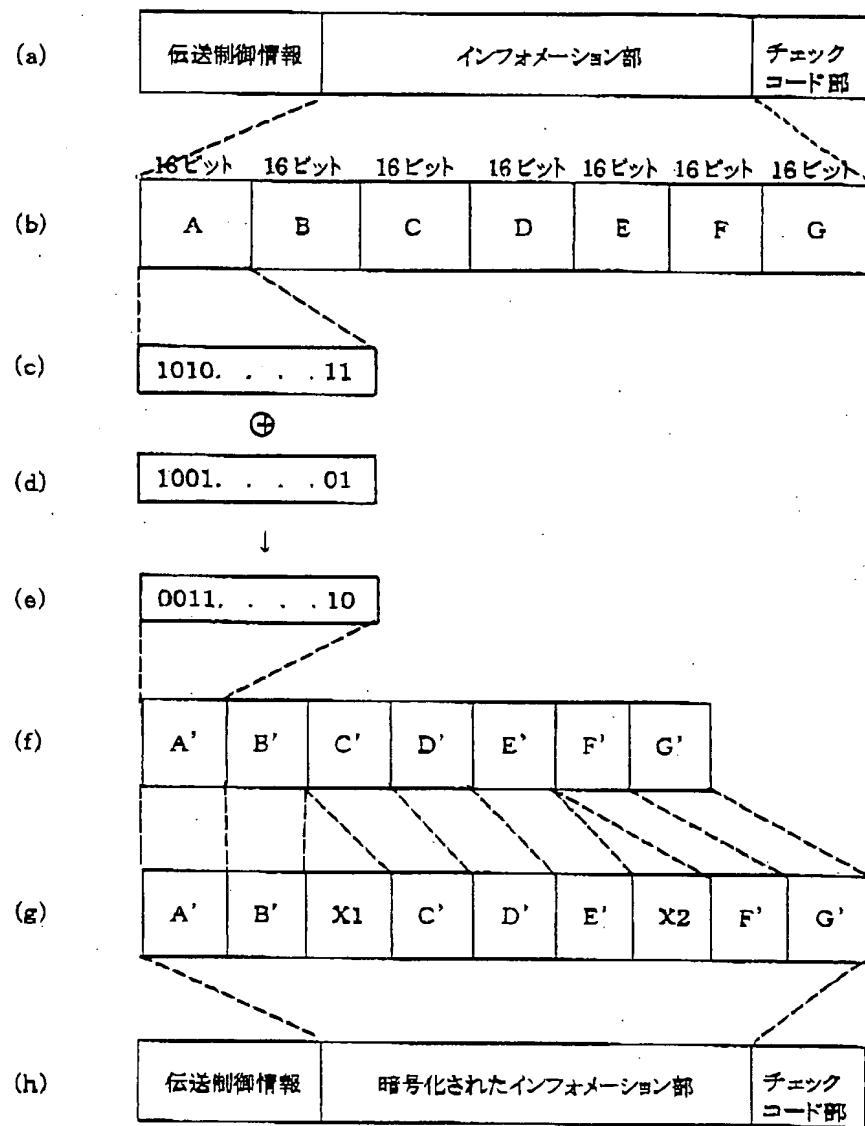
【図17】

アプリケーション	法則指定情報	暗号化の要否
クレジットカード	3	要
ポイントカード	1	否
プリペイドカード	5	否

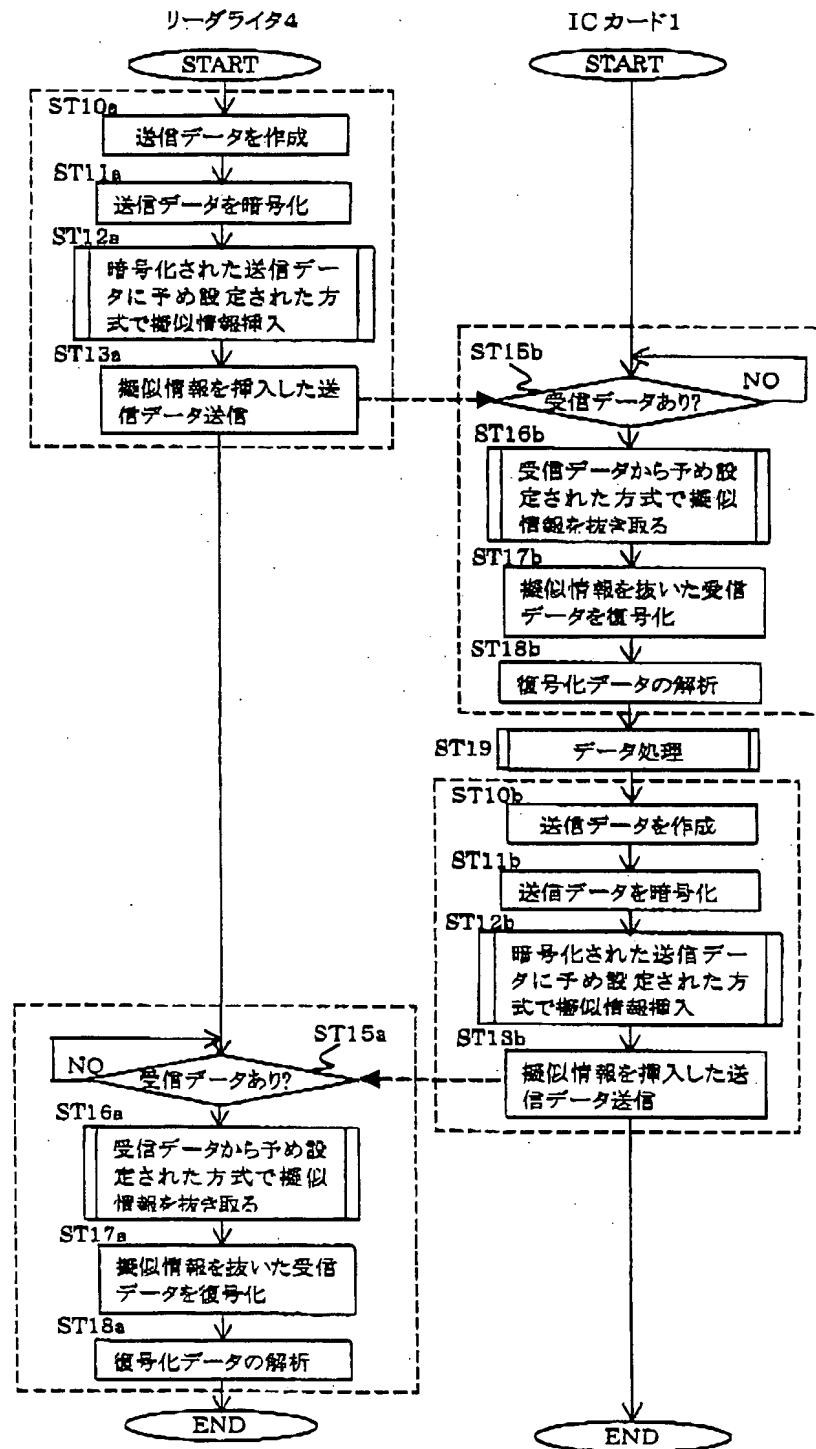
(14)

特開2002-111660

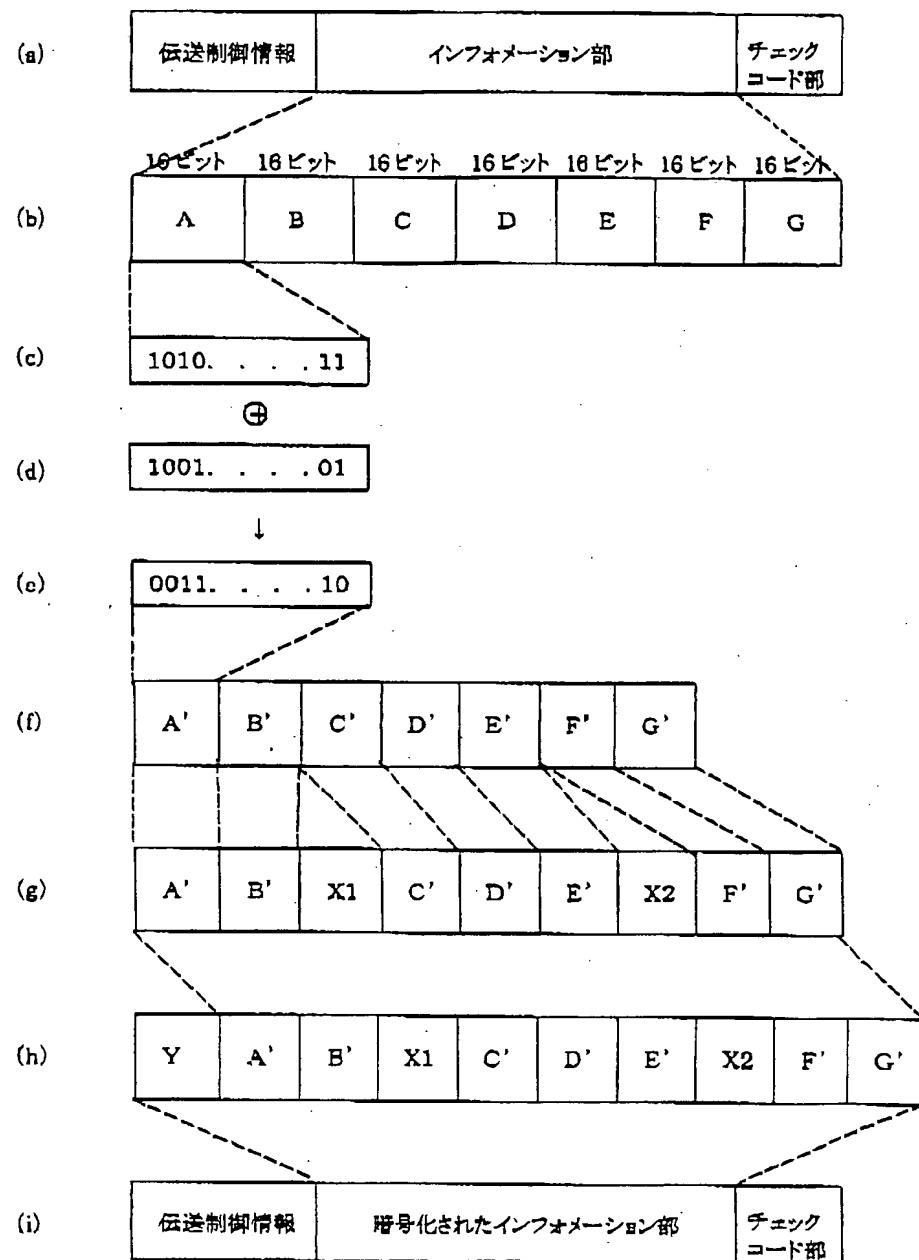
【図7】



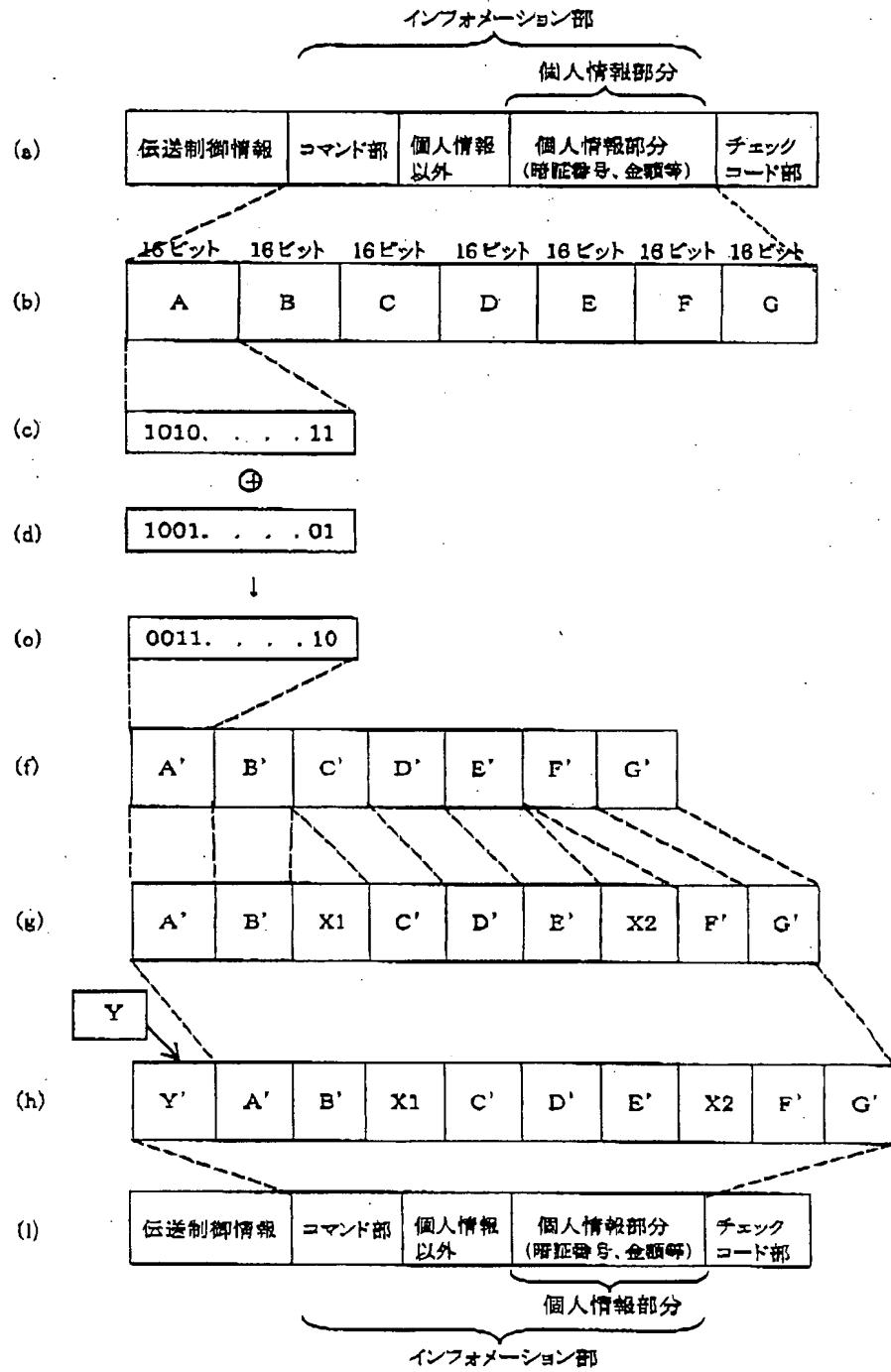
【図8】



【図9】



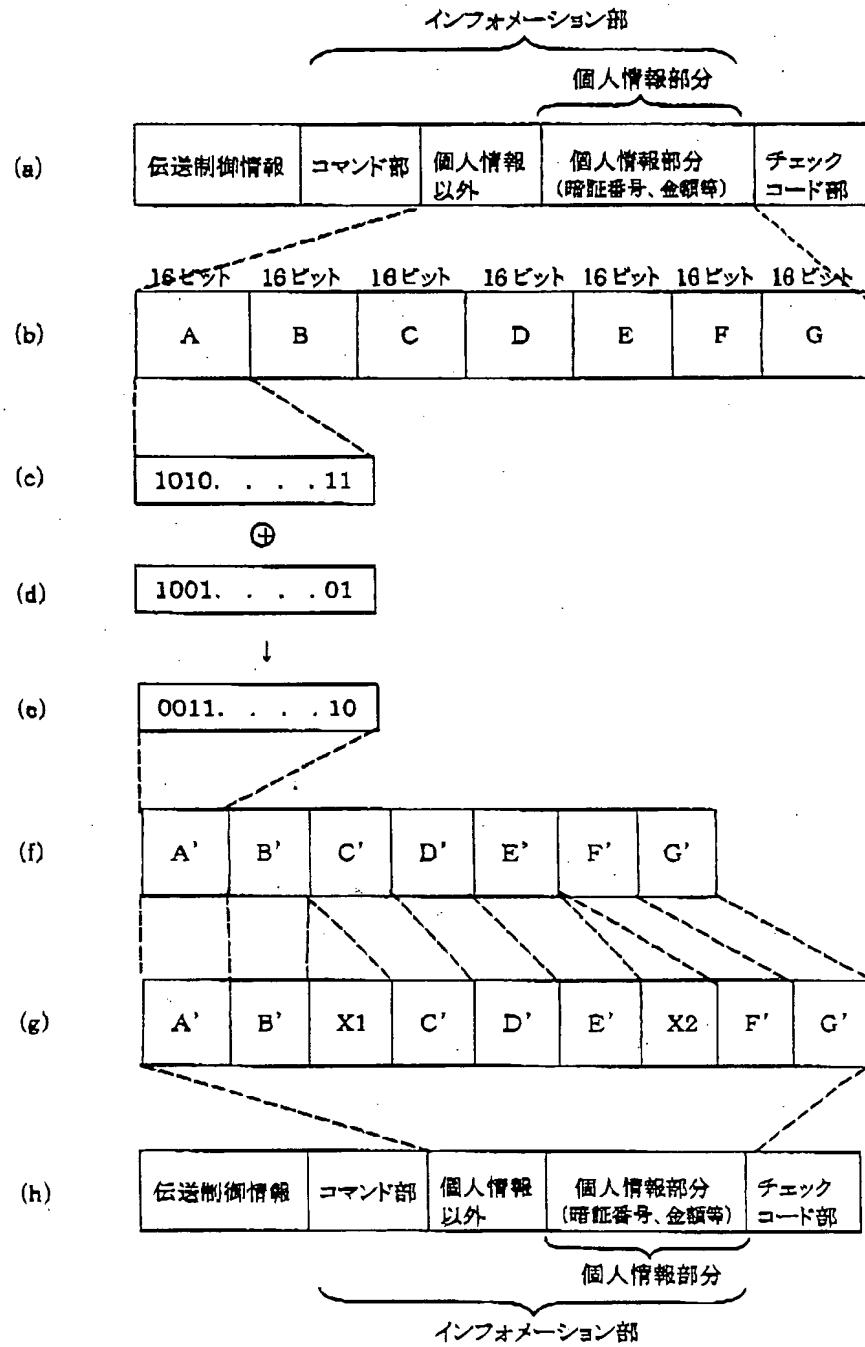
【図11】



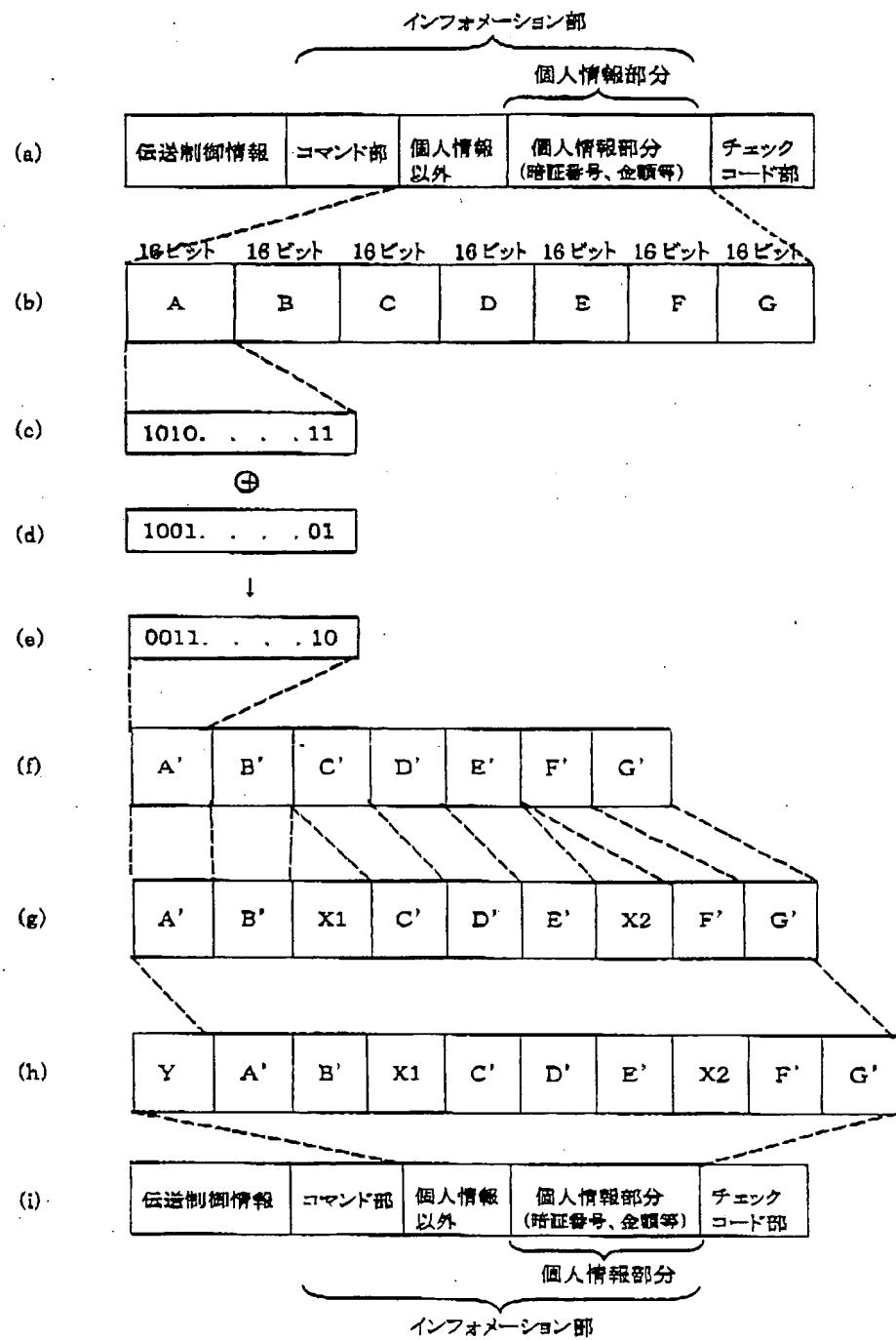
(18)

特開2002-111660

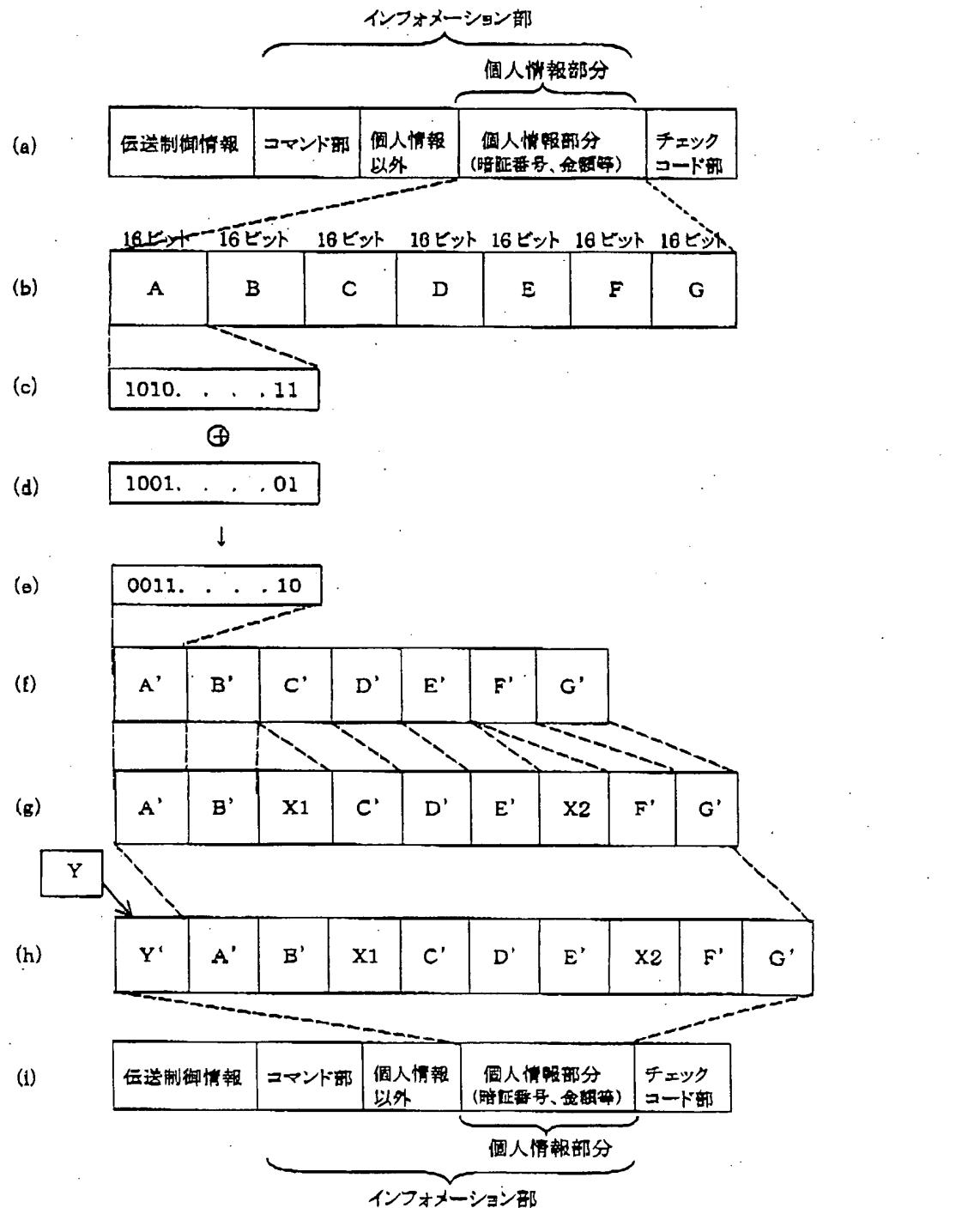
【図12】



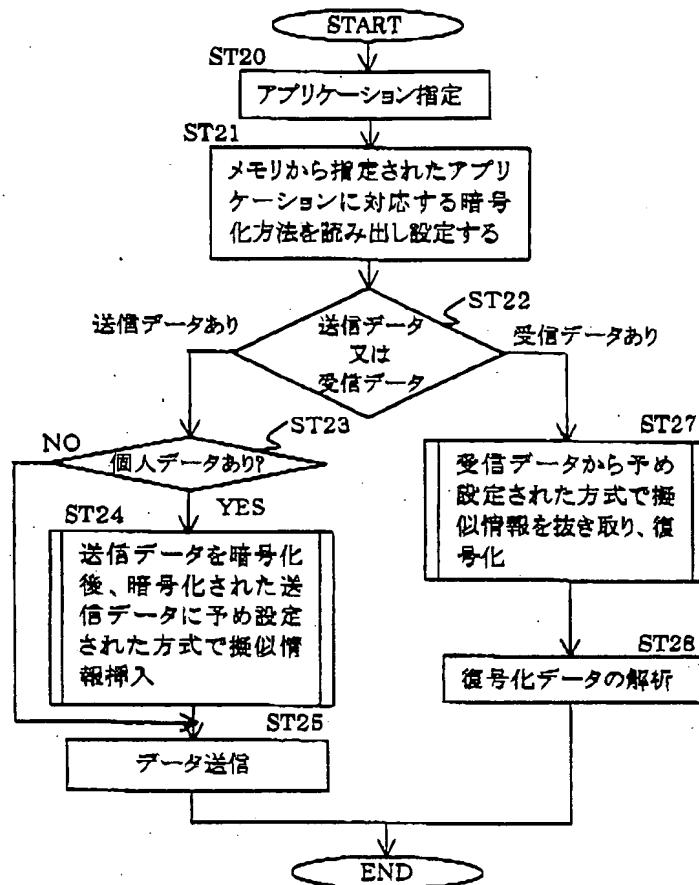
【図19】



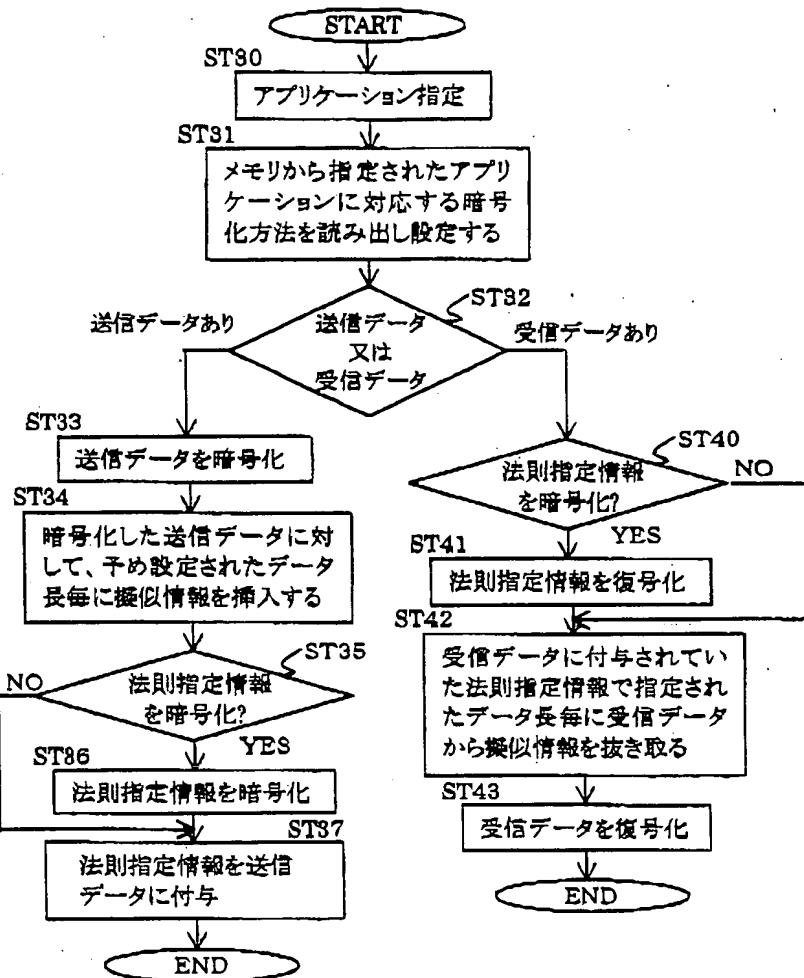
【図14】



【図16】



【図18】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.